

ORIGINAL

DOCKET FILE COPY ORIGINAL

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554**

RECEIVED

JUN 11 1996

FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF SECRETARY

In the Matter of

Implementation of the
Telecommunications Act of 1996:

Telecommunications Carriers' Use
of Customer Proprietary Network
Information and Other
Customer Information

)
)
)
)
)
)
)
)
)
)

CC Docket No. 96-115

**COMMENTS OF THE
ALARM INDUSTRY COMMUNICATIONS COMMITTEE**

Danny E. Adams
Steven A. Augustino
KELLEY DRYE & WARREN, LLP
1200 Nineteenth Street, N.W., Suite 500
Washington, D.C. 20036
202-955-9600

Its Attorneys

June 11, 1996

Noted for rec'd
JUN 11 1996

OTG

SUMMARY

In this proceeding, the Commission requests comment on rules to implement new Sections 275(d) and 222 of the Communications Act, as amended by the Telecommunications Act of 1996. These sections address two types of competitively-sensitive information -- customer proprietary network information ("CPNI") and data regarding the "occurrence or contents of calls" received by alarm monitoring providers -- which a LEC obtains solely as a result of its provision of local service. AICC supports the adoption of specific rules to prevent the LECs from misusing their access to this information.

Section 275(d) establishes a flat prohibition on the use for marketing purposes of the "occurrence or content of calls" to alarm providers. It applies to marketing on behalf of the LEC or any other entity, affiliated or unaffiliated, the LEC may choose to allow to access the data. The Commission should adopt a rule which is faithful to the statute's broad scope. It also should emphasize that the restrictions of Section 275 are in addition to the LEC's obligations under Section 222 and, in particular, that customer consent to access CPNI under Section 222 does *not* permit a LEC to use CPNI to market alarm monitoring services. Complaints alleging violations of Section 275(d) should be reviewed using expedited processing procedures.

Regarding Section 222, the Commission is correct that a carrier may not use CPNI derived from one service in order to market another service, unless it obtains prior customer approval. The Commission should clarify that CPNI may never be used to market alarm monitoring services or other enhanced services without prior customer approval. AICC believes all customer authorizations -- whether for LEC access or third-party access --

must be in writing and must be obtained after full disclosure of the customer's rights to protect this information. Finally, the Commission should narrowly construe the exceptions to customer approval contained in Section 222(d).

TABLE OF CONTENTS

SUMMARY	i
I. INTRODUCTION	1
II. RESTRICTIONS ON THE USE OF INFORMATION CONCERNING CALLS RECEIVED BY ALARM MONITORING SERVICE PROVIDERS	5
III. RESTRICTIONS ON THE USE OF CUSTOMER CPNI	7
CONCLUSION	12

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554**

In the Matter of)	
)	
Implementation of the)	CC Docket No. 96-115
Telecommunications Act of 1996:)	
)	
Telecommunications Carriers' Use)	
of Customer Proprietary Network)	
Information and Other)	
Customer Information)	

**COMMENTS OF THE
ALARM INDUSTRY COMMUNICATIONS COMMITTEE**

The Alarm Industry Communications Committee ("AICC"), by its attorneys, respectfully submits the following comments in response to the Commission's Notice of Proposed Rulemaking in the above-captioned docket.¹ For the reasons below, the AICC supports the adoption of rules to prevent incumbent local exchange carriers from misusing customer proprietary network information ("CPNI") and other data obtained as a result of their provision of local exchange services.

I. INTRODUCTION

AICC is a subcommittee of the Central Station Alarm Association. Its members consist of ADT Security Systems, Inc.; Holmes Protection Group; Honeywell Protection Services; the National Burglar and Fire Alarm Association; Rollins, Inc.; Wells

¹ FCC 96-221 (rel. May 17, 1996) (*Notice*).

Fargo Alarm Services; the Security Industry Association and Security Network of America. The membership represented by the AICC constitutes the overwhelming majority of the alarm security services in the United States. AICC members are highly dependent on the Bell Operating Companies ("BOCs") and other local exchange carriers ("LECs") for essential services and interconnection to local exchange facilities in order to provide alarm monitoring services. AICC has participated extensively over the years in Commission proceedings affecting the provision of alarm monitoring services.

The alarm industry, like other industries which rely on local exchange services, has always been concerned about the potential for abuse engendered by LEC participation in adjacent competitive markets. While there are many ways that a LEC can exploit its unique position in local services, one area of particular importance is the use of data a LEC obtains solely as a result of providing local services to its subscribers. The LEC, simply because all but a tiny percentage of calls must pass through its facilities, is in possession of a substantial amount of competitively valuable customer-specific information which could be used to market LEC services, to identify a competitor's customers, or to discriminate against its competitors. A LEC's access to this information raises concerns over the protection of customer privacy and over the protection of competition in telecommunications and adjacent markets, such as enhanced services.

The opportunities for LEC abuse of this information in the alarm services market are substantial. It would not be very difficult for a LEC to target alarm customers using information it receives in the ordinary course of its provision of local services. For example, some alarm equipment is programmed to contact the alarm provider's central

station at regular intervals (usually once per day) and every alarm customer has, on average, at least one alarm signal per year (whether it is a real alarm condition or a false alarm). As a result, using a list of telephone numbers alarm providers employ for these purposes, a LEC could canvass its customers' outbound call records to identify customers of alarm monitoring services. These customers could then become targets for the marketing of a LEC's alarm services (or those of a preferred alarm provider). Or, alternatively, the LEC could capture customer telephone numbers from records of the incoming calls received by an alarm provider. By pursuing such actions, a LEC would know not only which customers use alarm services, but which provider they are using and the frequency of the customer's alarm conditions. In addition to gaining information on potential customers, such actions would enable the LEC to gain valuable insights into its competitors, such as the size of their customer base or the geographic scope of their business.

Indeed, alarm providers are especially vulnerable to such abuse because, as a practical matter, they are totally dependent upon the incumbent LECs to provide a service essential to the provision of alarm monitoring. Alarm monitoring services require, in addition to other capabilities, the ability to transmit information from the customer's location to an alarm monitoring provider's facilities.² The single most common arrangement for receiving this information is the use of the public switched telephone network on a per call basis. For customers with special security needs, however, private line connections or

² Among the purposes for which alarm monitoring providers receive information from a customer's premises are to identify when a premise goes to an "active" condition, to perform routine line-integrity verification, and to signal when a specified alarm or fire condition exists.

derived local channel technology³ may be used, separately or in combination with reliance on the public switched telephone network, to provide this essential communications link between the customer premises and the alarm provider. In most alarm installations, LEC facilities provide the means of transmitting this information. Bypass of these facilities typically is not technically feasible or is impractical from the customer's perspective. As a result, the alarm industry is in the uneasy position of relying on a potential competitor for an essential component of its business.⁴

It is for these reasons that Congress concluded the potential for LEC anticompetitive activities in the provision of alarm monitoring services is "real ... not theoretical."⁵ In Sections 222 and 275(d), Congress responded to these concerns by prohibiting the LECs from abusing their unique access to data generated in the provision of local exchange services.

³ Derived local channel technology employs a "data over voice" transmission to permit supervision of the integrity of a line linked to the public switched network.

⁴ The advent of multiple local service providers, as envisioned by the Telecommunications Act of 1996, will not materially alter the alarm industry's dependence upon local service providers. The presence of multiple local service providers will increase customer choice in obtaining local service, but in most instances alarm providers will be limited to the use of whichever local service provider is chosen by the customer for his or her local calling needs.

⁵ See H.R. Rep. No. 104-204, 104th Cong., 1st Sess. 87 (1995). In response to this danger, Congress prohibited the BOCs from entering the market for five years. See 47 U.S.C. § 275(a).

II. **RESTRICTIONS ON THE USE OF INFORMATION CONCERNING CALLS RECEIVED BY ALARM MONITORING SERVICE PROVIDERS**

Section 275(d) states that a LEC "may not record or use in any fashion the occurrence or contents of calls received by providers of alarm monitoring services for the purposes of marketing such services on behalf of [the LEC] or any other entity."⁶ This provision establishes a flat prohibition on the use of information regarding the "occurrence or contents of calls" to alarm providers for *any* marketing purpose. The restriction applies to the LEC itself and also to any entity, affiliated or unaffiliated, that might be given access to the data. Thus, not only is a LEC prohibited from using the information to market services on its own behalf, but it also is prohibited from selling customer data to third parties.

The Commission is correct that authorization received from customers to access CPNI does *not* enable the LEC to engage in marketing based upon data reflecting the occurrence or contents of calls to alarm providers.⁷ Although the data covered by Section 275(d) may sometimes include information which also meets the definition of CPNI, AICC agrees with the Commission that Section 275(d) data is broader in scope.⁸ Section 275(d) applies to the contents of a call, in addition to records identifying the occurrence of a call to an alarm provider. Section 275(d) also applies to data even where it is associated with the alarm provider's use of the local network (and therefore is the provider's CPNI, not the customer's), or where it is not the CPNI of any particular customer.

⁶ 47 U.S.C. § 275(d).

⁷ *Notice*, at ¶ 47.

⁸ *Id.*

Moreover, even where there is overlap in these definitions, Sections 275(d) and 222 should be read as independent obligations, both of which are applicable. Nothing in the statute would support an interpretation that limits the scope of either Section 222 or Section 275(d). They must be read as independent, and cumulative, obligations of LECs. Thus, while customer consent pursuant to Section 222 might permit the use of customer calling data for some purposes, it does not override Section 275(d)'s separate restriction on using the information for the marketing of alarm services.

More fundamentally, Section 275(d) cannot be waived by the customer making a call. Unlike Section 222, there is no customer approval provision in Section 275(d). The statute prohibits the use of call data for marketing of alarm services under all circumstances, without exception. Thus, even if a customer consents to the use of his or her CPNI, that consent cannot be construed to negate the protection of Section 275(d).⁹ The LEC is obligated to ensure that, with or without consent to use CPNI, data regarding calls to alarm service providers are not misused for marketing purposes.

The restrictions of Section 275(d) are self-effectuating. That is, they do not require the Commission to issue a rule before the LEC is subject to the obligation. Nevertheless, if the Commission adopts a rule implementing Section 275(d), that rule should be faithful to the statute's broad scope and should emphasize that the Section 275(d) obligations are independent of and in addition to, any other obligations imposed under Section 222 or other applicable law. In addition, in order to ensure that data subject to Section 275(d) is not improperly disclosed as CPNI, the Commission should require LECs to

⁹ Similarly, the exceptions to CPNI approval contained in Section 222 do not excuse the LEC from compliance with Section 275(d). *See* 47 U.S.C. § 222(d).

deny access to CPNI to any LEC personnel (or personnel of an affiliate) that have responsibility for the marketing of alarm monitoring services.¹⁰

Finally, the Commission should adopt expedited procedures for the processing of complaints alleging violations of Section 275(d). Section 275(d) violations implicate the same competitive concerns as do violations of Section 275(b), for which Congress mandated expedited complaint processing. In particular, the abuse of alarm data is likely to present immediate and irreparable harm to the aggrieved alarm monitoring provider. Therefore, the Commission should exercise its enforcement discretion to expedite the processing of complaints by alarm monitoring service providers concerning violations of Section 275(d).

III. RESTRICTIONS ON THE USE OF CUSTOMER CPNI

In addition to the new restrictions on the use of alarm monitoring data, the 1996 Act adds a new Section 222 to the Communications Act, as amended. This section creates a duty of all telecommunications carriers to protect the confidentiality of customer information. Under Section 222, a telecommunications carrier may not use CPNI for any purpose other than to provide "the telecommunications service from which such information is derived" or services necessary to provide that service, unless it has first obtained the approval of the customer.¹¹

¹⁰ The Commission could consider a waiver of this requirement if the LEC can demonstrate it adequately screens Section 275(d) data from other CPNI made available to these individuals.

¹¹ 47 U.S.C. § 222(c)(1). Customer approval also is not necessary in the circumstances described in Section 222(d). 47 U.S.C. § 222(d).

Initially, the Commission is correct that "nothing in the 1996 Act affects" other restrictions which may apply to CPNI.¹² Thus, as explained in the preceding section, the restrictions imposed in Section 275(d) apply in addition to the obligations of Section 222. Further, the Commission should retain its *Computer III* restrictions on the BOCs' use of CPNI, except where Section 222 explicitly imposes a different obligation upon the BOCs. These restrictions on CPNI were adopted by the Commission pursuant to separate authority and were based upon a conclusion that they were in the public interest to protect against access discrimination by BOCs engaged in the provision of enhanced services. These concerns remain as valid today as they were then. Indeed, AICC believes the record in *Computer III* justified even greater restrictions on access to CPNI than the Commission adopted. Nothing in the passage of the Act, therefore, should provide a basis to retreat from those restrictions.

The only area where the *Computer III* restrictions should be modified is where a specific obligation of Section 222 conflicts with the *Computer III* rules. For example, Section 222 does not permit the BOCs to have presumptive access to customer CPNI for any marketing purposes. Thus, the Act overrides the Commission's decision in *Computer III* to permit the BOCs automatically to access the CPNI of customers with 20 or fewer lines.¹³ The Commission should modify its *Computer III* rules to eliminate the presumptive access the BOCs enjoyed to the CPNI of certain customers.

¹² Notice, at ¶ 38.

¹³ See *Computer III Remand Proceedings: Bell Operating Company Safeguards and Tier 1 Local Exchange Company Safeguards*, 6 FCC Rcd 7571 (1991).

Second, AICC agrees with the Commission that Section 222 is intended to prevent LECs from using information gained as a result of providing one telecommunications service to market a different service. U S West's argument that the Act gives carriers *carte blanche* to use CPNI to market any telecommunications service if they offer one telecommunications service (*Notice*, ¶ 20) would render Section 222 a meaningless prohibition on the disclosure of usage information to third parties. This could not have been what Congress intended in enacting Section 222, and the Commission is correct in rejecting U S West's argument.¹⁴

AICC endorses the Commission's attempt to define the limit of permissible uses of CPNI with respect to the service categories traditionally applied in the past.¹⁵ The Commission should make explicit in its rule that enhanced services do not fall within the local service category described in the *Notice*. Alarm monitoring services are not "local" services, and a LEC should not be permitted to use CPNI to market such services without first obtaining customer approval. Indeed, since enhanced services are not basic telecommunications services at all, a carrier should not be permitted to use CPNI to market any enhanced service without obtaining prior customer approval.¹⁶

Third, AICC believes that written customer approval should be required for a LEC to access customer CPNI. Section 222(c)(1) requires a LEC to obtain "the approval of the customer" before using CPNI for any marketing purposes. Written approval is the most

¹⁴ *Notice* at ¶ 20.

¹⁵ *Id.* at ¶ 22.

¹⁶ *See id.* at ¶ 26.

reliable form of approval and is the easiest to verify in the event of a dispute. It is, as the Commission notes, preferable to oral authorization.¹⁷ To ensure that any written authorization is knowing and intentional, the Commission should require LECs to give notification to customers of their CPNI rights, including the right to grant access to third parties.¹⁸

Neither Section 222(c)(2) nor Section 222(d)(3) supports a contrary conclusion. Section 222(c)(2) establishes written authorization as the method for disclosure of CPNI "to *any person* designated by the customer."¹⁹ The use of the term "any person," rather than a more restrictive term, such as "a third party," implies that the provision applies to disclosure to the LEC as well as to third parties.²⁰

Section 222(d)(3) also is consistent with a written authorization requirement. Section 222(d)(3) allows a LEC to use CPNI to provide inbound telemarketing if the customer approves the disclosure. As a practical matter, such approval will necessarily be oral, as that is the only feasible method of obtaining authorization on an inbound call. The fact that this type of authorization is limited both in scope (only for calls "initiated by the customer") and in duration (only for the length of the call) supports the inference that

¹⁷ *Id.* at ¶ 29.

¹⁸ Such notification must be in accordance with FCC-prescribed form and content requirements and should occur at least once per year.

¹⁹ 47 U.S.C. § 222(c)(2) (emphasis added).

²⁰ Use by the LEC of CPNI is itself a "disclosure," since LEC personnel must receive the information in order to make use of it. *Cf.* 47 U.S.C. § 222(c)(1) (allowing a LEC to "use, disclose or permit access to" CPNI only in the provision of the telecommunications service from which the information is derived).

Congress viewed oral authorization as inherently suspect. Moreover, if Congress had contemplated that oral authorization could permit access to CPNI in other instances, there would be no reason to limit the duration of a customer's authorization on an inbound call, since a customer could legitimately consent to authorization for a longer duration. Accordingly, read as a whole, Section 222 requires written approval for the disclosure of CPNI to the LEC as well as to third parties.²¹

Fourth, the exceptions to customer approval contained in Section 222(d) should be narrowly construed. In particular, the Commission should strictly limit the applicability of Section 222(d)(3) to inbound calls in which the customer initiates the call *and* initiates a discussion of enhanced services or other services for which access to CPNI is useful. The inbound call exception does not authorize LECs to bombard all callers with CPNI approval requests every time they attempt to contact their LEC with a question or service complaint. The exception should be limited to situations where the LEC is responding to the customer's initiative. Moreover, the Commission should specify that customer approval to use CPNI on inbound calls must be explicit and affirmative; the LEC may not infer approval from the fact that a customer remains on the line after being given a CPNI approval "request." Customer approval must be knowing and intentional, after disclosure by the LEC that the customer may limit access to such information if he or she wishes. Finally, the Commission must

²¹ As the Commission has done in the past, it should review the LECs' proposed authorization forms and should specify the minimum content they must contain. *See BOC ONA Amendment Order*, 5 FCC Rcd 3103, 3120, 3133 n.264 (1990). This procedure is consistent with the Commission's approach to "letters of agency" to authorize changes in long distance carriers, where the Commission has specified the minimum form and content requirements for such documents. *See Policies and Rules Concerning Unauthorized Changes in Long Distance Carriers*, 10 FCC Rcd 9560 (1995).

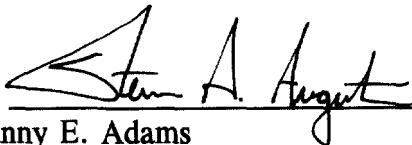
strictly limit CPNI access to the duration of the call. Nothing in the Act permits a LEC to grant access to CPNI for follow-up purposes after the call. Only affirmative written authorization may permit access after the call is completed.

CONCLUSION

For the foregoing reasons, AICC recommends that the Commission adopt rules to prevent LECs from misusing alarm monitoring data and customer proprietary network information to gain an unfair advantage in their provision of other telecommunications and enhanced services. The obligations of Section 275(d) and of Section 222 apply independently, and a LEC must satisfy each section (in addition to other applicable law) prior to using such data for marketing purposes.

Respectfully submitted,

**ALARM INDUSTRY COMMUNICATIONS
COMMITTEE**

By  _____

Danny E. Adams

Steven A. Augustino

KELLEY DRYE & WARREN, LLP

1200 Nineteenth Street, N.W., Suite 500

Washington, D.C. 20036

202-955-9600

Its Attorneys

June 11, 1996